GRC RFP QUESTIONNAIRE

1. Company Overview & Market Leadership

How many years has your company provided Governance, Risk & Compliance (GRC) solutions?

How many customers use GRC/Compliance modules?

In which industries or regions do you have the strongest presence?

What independent analysts or awards recognize your company as an industry leader?

What global standards and frameworks does your solution align with (e.g., ISO 37301, COSO, DOJ guidance)?

How long have your Governance, Risk & Compliance (GRC) modules operated as a unified platform rather than standalone products?

How does your GRC solution integrate with third-party systems for policy, learning, or incident management?

2. Platform & Architecture

Is your solution part of a unified platform?

Can the platform be hosted in regional data centers to meet data residency requirements?

What integration options exist with HR, ERP, and third-party systems (APIs, connectors, SSO, etc.)?

Does the platform support configurable workflows without custom code?

What is your approach to platform scalability, uptime, and performance SLAs?

3. Functional Modules & Capabilities - Use this section to determine whether each key area is supported and configurable within the vendor's platform.

Enterprise Risk Management Capabilities

Can risks be captured, assessed, and linked to controls, incidents, and audits?

Are risk scoring models configurable by type, region, or business unit?

Can users define key risk indicators (KRIs) and monitor them dynamically?

Can risk data be rolled up into enterprise-level views for executive reporting?

How are risks visualized in dashboards (heatmaps, trends, impact-probability)?

Regulatory Compliance/Regulatory Change Management Capabilities

Can regulatory obligations be tracked and mapped to internal policies and controls

Does the system support automated updates from external regulatory sources?

Can users assign ownership and monitor compliance against specific requirements?

How are testing results and control evidence captured and reported?

Can obligations and controls be linked to audit findings or remediation actions?

Incident Management Capabilities

Can incidents be logged and categorized by type, severity, and source?

Does the system automate routing and escalation through configurable workflows?

Can incidents be linked to risks, controls, or audit findings for root-cause analysis?

How are investigations documented and tracked to closure?

Are incident metrics and trends available in dashboards and reports?

Internal Audit Capabilities

Can audit plans, programs, and checklists be managed within the system?

Does the system automate routing and escalation through configurable workflows?

Can incidents be linked to risks, controls, or audit findings for root-cause analysis?

Does the platform provide standardized audit templates or libraries?

How are audit reports generated and distributed securely to stakeholders?
Internal Control Capabilities
Can controls be defined, categorized, and linked to risks and policies?
Does the platform support automated control testing and evidence capture?
Are control owners notified of testing schedules and remediation tasks?
Can dashboards track control performance and effectiveness over time?
How are failed controls escalated for review or corrective action?
Policy Management Capabilities
Can policies be created, reviewed, approved, and version-controlled in the system?
Are policies linked to related controls, risks, and training modules?
Can acknowledgements and attestations be tracked by user or group?
Does the workflow support multi-step approvals and publication scheduling?
How are policies distributed globally and tracked for compliance?
Third Party Risk Management Capabilities
Can vendors be onboarded, risk-assessed, and scored automatically?
Does the platform integrate with external due diligence data sources?
Can ongoing monitoring detect changes in supplier risk status?
Are corrective actions and follow-ups managed through automated workflows?
How are supplier risk dashboards configured for business units or regions?
Conflicts of Interest/Disclosure Management Capabilities
Can employees disclose potential or actual conflicts of interest digitally?
Are submissions routed for review and approval via configurable workflows?
Can conflicts be linked to policies or attestations for compliance tracking?
Are reminders and escalation rules available for pending reviews?
Are gift-giving and receiving limits enforced automatically by value, region, or recipient role?
Business Continuity Management Capabilities
Can business impact analyses (BIAs) and recovery strategies be created and updated?
Does the system support scenario planning and simulation testing?
Can continuity plans be linked to critical risks and assets?
Are notifications automated during exercises or actual events?
How is BCM performance reported to leadership and regulators?
Horizon Scanning Capabilities
Can you monitor global news sources to identify external or emerging risks?
Can changes in external risk be automatically flagged and linked to impacted controls, policies, risks, or training?
Can external intelligence be integrated directly into internal risk registers, controls and mitigation workflows?
Are dashboards available that visualise external threats and internal exposure side-by-side with drill-down capability (severity, trends, domains)?
Can your solution generate reports summarising regulatory changes, emerging risk themes, and their potential business impact over defined periods?
Whistleblower & Case Management Capabilities
How does the platform ensure confidentiality, protect anonymity, and comply with EU Whistleblower Directive and other global reporting laws?
Can reports automatically trigger configurable workflows for triage, investigation, and resolution?

Are cases tracked with attachments, audit trails, and documented outcomes?

Can employees submit reports through mobile devices or tablets, and is the interface optimized for mobile use?

Can submitted reports be automatically translated or reviewed in multiple languages for global case handling?

Ethics & Compliance Training

How extensive is your library of compliance and ethics courses (e.g., Code of Conduct, Anti-Bribery, Data Privacy, DEI & Respect, Cybersecurity, Third Party Risk, AI Ethics)?

What editing tools or authoring capabilities are provided for in-house content updates?

Can your content be deployed through an existing LMS or does it require a proprietary platform?

How many languages is your content available in?

Does the system support microlearning, multilingual content, and mobile access?

Can the platform deliver adaptive or personalized learning based on role, region, or prior knowledge?

4. Program Management Capabilities

How does the solution enable monitoring and testing of controls?

Can GRC assessments be scheduled, automated, and linked to risk registers?

Does the system support regulatory mapping to link controls and obligations?

How are corrective actions and remediation plans tracked?

Can managers assign accountability and track attestations or policy acknowledgments?

Are dashboards and reports configurable by user role and audience?

5. Regulatory Intelligence & Change Management

How are regulatory obligations tracked and updated?

Do you provide built-in regulatory content or horizon scanning to identify new or changing requirements?

How can users link regulations to internal policies, controls, and risks?

Can you demonstrate how the system supports evidence collection for audits or investigations?

6. Risk Integration & Reporting

Can risks be linked to enterprise risks, controls, and incidents within the same platform?

What analytics and visualizations are available to demonstrate compliance effectiveness to leadership?

Does the solution support automated workflows for issue escalation and remediation?

Can reporting be configured for different stakeholders (board, audit committee, business unit leaders)?

What options exist for continuous monitoring or AI-assisted trend detection?

7. Security, Privacy & Data Governance

How is client data secured at rest and in transit?

Is your hosting environment certified under ISO 27001, SOC 2 Type II, or equivalent frameworks?

How do you ensure compliance with GDPR and other data protection laws?

Are customer environments logically segregated from other clients?

Do you offer audit trails, access logs, and granular permission controls?

8. Implementation, Services & Support

What is your typical implementation timeline?

Do you provide configuration support or managed services?

How are customers supported post-go-live (CSM, technical support, advisory)?
What training resources and knowledge bases are available to administrators and users?
How often are platform updates and enhancements released?
9. Innovation & Roadmap
How are emerging technologies like AI, machine learning, and automation integrated into your roadmap?
How do you prioritize enhancements based on customer feedback?
What differentiates your product vision for compliance program maturity over the next 3–5 years?
10. Commercials & Value
How is pricing structured (modular, user-based, or enterprise license)?
What services and support are included in annual fees?
Are updates and new content releases included or charged separately?
Can the solution scale cost-effectively as our compliance program grows?
11. References & Proof of Success
Can you provide customer success stories demonstrating measurable improvements?
What metrics or KPIs do your clients typically achieve post-implementation?
What is your customer retention rate for Risk solutions?